1. (Currently Amended) A data transmitting system comprising a portable optical disc ~~data recording~~ medium and a drive unit which accesses the portable optical disc ~~data recording~~ medium,

the portable optical disc ~~data recording~~ medium including:

a security module comprising a nonvolatile memory which executes a mutual authentication protocol with the drive unit; and

~~a storage area~~ an optical disc distinct from the security module; and

the drive unit including:

a controller which executes the mutual authentication protocol when accessing the portable optical disc ~~data recording~~ medium; and

an interface unit which accesses the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium.

2. (Previously Presented) The system as set forth in Claim 1, wherein the mutual authentication protocol uses public-key encryption technology.

3. (Canceled)

4. (Currently Amended) The system as set forth in Claim 3, wherein the drive unit further includes means for driving the optical disc.

5. (Currently Amended) The system as set forth in Claim 1, wherein the interface unit accesses the optical disc ~~storage area~~ directly.

6. (Canceled)

7. (Currently Amended) The system as set forth in Claim 1, wherein the interface unit accesses the optical disc ~~storage area~~ via the security module.

8. (Canceled)

9. (Currently Amended) The system as set forth in Claim 1, wherein identification data of the portable optical disc ~~data recording~~ medium is stored in the security module.

10. (Previously Presented) The system as set forth in Claim 1, wherein the security module stores a revocation list of illegal drive units.

11. (Currently Amended) The system as set forth in Claim 1, wherein the optical disc ~~storage area~~ stores a revocation list of illegal drive units.

12. (Previously Presented) The system as set forth in Claim 1, wherein the drive unit stores a revocation list of illegal recording media.

13. (Previously Presented) The system as set forth in Claim 1, wherein the drive unit does not store a revocation list of illegal recording media.

14. (Currently Amended) The system as set forth in Claim 1, wherein the mutual authentication protocol executes independently of whether the drive unit or the portable optical disc ~~data recording~~ medium contains an illegal unit revocation list.

15. (Previously Presented) The system as set forth in Claim 1, wherein the controller of the drive unit judges whether or not the security module has an illegal unit revocation list stored therein, and executes the mutual authentication protocol based on the judgment.

16. (Canceled)

17. (Currently Amended) The system as set forth in Claim 1, wherein:

the portable optical disc ~~data recording~~ medium stores therein a first version of an illegal unit revocation list and a first list version number;

the drive unit stores therein a second version of the illegal unit revocation list and a second list version number; and

the portable optical disc ~~data recording~~ medium and the drive unit exchange the first and second version numbers when executing the mutual authentication protocol, and whichever has a newer version of the illegal unit revocation list sends the newer version of the illegal unit revocation list to the other.

18. (Currently Amended) The system as set forth in Claim 17, wherein:

the portable optical disc ~~data recording~~ medium has the first list version number and the first version of the illegal unit revocation list stored in the optical disc ~~storage area~~;

the drive unit comprises a storage unit and stores the second list version number and the second version of the illegal unit revocation list stored in the storage unit;

the security module of the portable optical disc ~~data recording~~ medium and controller of the drive unit exchange the first version number and the second version number when executing the mutual authentication protocol; and

the portable optical disc ~~data recording~~ medium and drive unit exchange the list with the newer version number.

19. (Previously Presented) The system as set forth in Claim 1, wherein the drive unit checks a second version of an illegal unit revocation list to authenticate the security module and the security module checks a first version of the illegal unit revocation list to authenticate the drive unit.

20. (Previously Presented) The system as set forth in Claim 17, wherein:

the drive unit further stores identification data; and

the security module receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal

unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the drive unit is revoked.

21. (Currently Amended) The system as set forth in Claim 17, wherein:

the portable optical disc ~~data recording~~ medium stores identification data; and

the controller of the drive unit receives the identification data from the security module and checks whether or not the identification data of the portable optical disc ~~data recording~~ medium is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the portable optical disc ~~data recording~~ medium is revoked.

22. (Previously Presented) The system as set forth in Claim 17, wherein the illegal unit revocation list includes identification data of revoked units.

23. (Previously Presented) The system as set forth in Claim 17, wherein the illegal unit revocation list identifies units that have not been revoked.

24. (Previously Presented) The system as set forth in Claim 17, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

25. (Previously Presented) The system as set forth in Claim 17, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

26. (Previously Presented) The system as set forth in Claim 1, wherein when executing the mutual authentication protocol, the drive unit and the security module execute a key sharing protocol using public-key encryption technology, encrypt a content key with a shared key, and transfer the encrypted content key.

27. (Previously Presented) The system as set forth in Claim 1, wherein when executing the mutual authentication protocol, the drive unit and the security module execute a key sharing protocol using public-key encryption technology, encrypt data with a shared key, and transfer the encrypted data.

28. (Currently Amended) The system as set forth in Claim 1, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium via the interface unit;

the drive unit and the security module execute a key sharing protocol using public-key encryption technology;

the drive unit encrypts a content key with a shared key and sends the encrypted content key to the security module; and

the security module decrypts the encrypted content key, re-encrypts the decrypted content key with a save key stored therein and sends the re-encrypted content key to the drive unit; and

the drive unit writes to the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium the data encrypted with the content key and the content key encrypted by the save key.

29. (Currently Amended) The system as set forth in Claim 1, wherein:

the drive unit is to read data from the optical disc ~~storage area~~ via the interface unit;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the drive unit reads the encrypted content key from the optical disc ~~storage area~~ and sends the content key to the security module;

the security module decrypts the encrypted content key received from the drive unit with a save key stored therein, re-encrypts the decrypted content key with the shared key and sends the re-encrypted content key to the drive unit; and

the drive unit decrypts the encrypted content key received from the security module with the shared key, reads the content key-encrypted data from the optical disc ~~storage area~~ and decrypts the data.

30. (Currently Amended) The system as set forth in Claim 1, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and the security module execute a key sharing protocol using public-key encryption technology;

the drive unit sends to the security module a content key encrypted with a shared key, and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key and records to the optical disc ~~storage area~~ the content key re-encrypted with a save key stored in the security module and data encrypted with the content key received from the drive unit.

31. (Currently Amended) The system as set forth in Claim 1, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the drive unit encrypts data with a shared key and sends the data thus encrypted to the security module; and

the security module decrypts the encrypted data received from the drive unit with the shared key, encrypts the decrypted data and stores the encrypted data into the optical disc ~~storage area~~.

32. (Currently Amended) The system as set forth in Claim 1, wherein:

the drive unit is to read data from the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the security module reads from the optical disc ~~storage area~~ an encrypted content key and data encrypted with the content key, decrypts the encrypted content key with a save key stored therein and sends to the drive unit the content key re-encrypted with a shared key and data encrypted with the content key read from the optical disc ~~storage area~~; and

the drive unit decrypts the encrypted content key received from the security module with the shared key and decrypts the encrypted data with the content key.

33. (Currently Amended) The system as set forth in Claim 1, wherein:

the drive unit is to read data from the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the security module reads data encrypted and stored in the portable optical disc ~~data recording~~ medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit; and

the drive unit decrypts, with the shared key, the encrypted data received from the security module.

34. (Currently Amended) A data transmitting method comprising:

executing a mutual authentication protocol between a drive unit and a portable optical disc ~~data recording~~ medium, the portable optical disc ~~data recording~~ medium including a security module comprising a nonvolatile memory and [[a]] an optical disc ~~storage area~~ distinct from the security module; and

accessing, by the drive unit, the optical disc ~~storage area~~ distinct from the security module,

wherein the mutual authentication protocol is executed by communicating with the security module of the portable optical disc medium.

35. (Previously Presented) The method as set forth in Claim 34, wherein the mutual authentication protocol uses public-key encryption technology.

36. (Currently Amended) The method as set forth in Claim 47, wherein the drive unit accesses the optical disc ~~storage area~~ directly.

37. (Currently Amended) The method as set forth in Claim 34, wherein the drive unit accesses the optical disc ~~storage area~~ via the security module.

38. (Canceled)

39. (Currently Amended) The method as set forth in Claim 34, wherein identification data of the portable optical disc ~~data recording~~ medium is stored in the security module.

40. (Previously Presented) The method as set forth in Claim 34, wherein the security module stores a revocation list of illegal drive units.

41. (Currently Amended) The method as set forth in Claim 34, wherein the optical disc ~~storage area~~ stores a revocation list of illegal drive units

42. (Previously Presented) The method as set forth in Claim 34, wherein the drive unit stores a revocation list of illegal recording media.

43. (Previously Presented) The method as set forth in Claim 34, wherein the drive unit does not store a revocation list of illegal recording media.

44. (Currently Amended) The method as set forth in Claim 34, wherein a mutual authentication protocol executes independently of whether the drive unit or the portable optical disc ~~data recording~~ medium contains an illegal unit revocation list.

45. (Previously Presented) The method as set forth in Claim 34, wherein the drive unit judges whether or not the security module has an illegal unit revocation list stored therein, and executes the mutual authentication protocol based on the judgment.

46. (Canceled)

47. (Currently Amended) The method as set forth in Claim 34, wherein:

the portable optical disc ~~data recording~~ medium stores therein a first version of an illegal unit revocation list and a first list version number;

the drive unit stores therein a second version of the illegal unit revocation list and a second list version number; and

the optical disc ~~data recording~~ medium and the drive unit exchange the first and second version numbers when executing the mutual authentication protocol, and whichever has a newer version of the illegal unit revocation list sends the newer version of the illegal unit revocation list to the other.

48. (Currently Amended) The method as set forth in Claim 34, wherein:

the portable optical disc ~~data recording~~ medium has the first list version number and the first version of the illegal unit revocation list stored in the optical disc ~~storage area~~;

the drive unit comprises a storage unit and stores the second list version number and the second version of the illegal unit revocation list stored in the storage unit;

the security module of the portable optical disc ~~data recording~~ medium and controller of the drive unit exchange the first version number and the second version number when executing the mutual authentication protocol; and

the portable optical disc ~~data recording~~ medium and drive unit exchange the list with the newer version number.

49. (Previously Presented) The method as set forth in Claim 34, wherein the drive unit checks the second version of the illegal unit revocation list to authenticate the security module and the security module checks the first version of the illegal unit revocation list to authenticate the drive unit.

50. (Previously Presented) The method as set forth in Claim 47, wherein:

the drive unit further stores identification data; and

the security module receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the drive unit is revoked.

51. (Currently Amended) The method as set forth in Claim 47, wherein:

the portable optical disc ~~data recording~~ medium stores identification data; and

the drive unit receives the identification data from the security module and checks whether or not the identification data of the portable optical disc ~~data recording~~ medium is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the portable optical disc ~~data recording~~ medium is revoked.

52. (Previously Presented) The method as set forth in Claim 34, wherein the illegal unit revocation list includes identification data of revoked units.

53. (Previously Presented) The method as set forth in Claim 34, wherein the illegal unit revocation list identifies units that have not been revoked.

54. (Previously Presented) The method as set forth in Claim 34, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

55. (Previously Presented) The method as set forth in Claim 34, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

56. (Previously Presented) The method as set forth in Claim 34, wherein when executing the mutual authentication protocol, the drive unit and the security module execute a key sharing protocol using public-key encryption technology, encrypt a content key with a shared key, and transfer the encrypted content key.

57. (Previously Presented) The method as set forth in Claim 34, wherein when executing the mutual authentication protocol, the drive unit and the security module execute a key sharing protocol using public-key encryption technology, encrypt data with a shared key, and transfer the encrypted data.

58. (Currently Amended) The method as set forth in Claim 34, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium via the interface unit;

the drive unit and the security module execute a key sharing protocol using public-key encryption technology;

the drive unit encrypts a content key with a shared key and sends the encrypted content key to the security module; and

the security module decrypts the encrypted content key, re-encrypts the decrypted content key with a save key stored therein and sends the re-encrypted content key to the drive unit; and

the drive unit writes to the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium the data encrypted with the content key and the content key encrypted by the save key.

59. (Currently Amended) The method as set forth in Claim 34, wherein:

the drive unit is to read data from the optical disc ~~storage area~~ via the interface unit;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the drive unit reads the encrypted content key from the optical disc ~~storage area~~ and sends the content key to the security module;

the security module decrypts the encrypted content key received from the drive unit with a save key stored therein, re-encrypts the decrypted content key with the shared key and sends the re-encrypted content key to the drive unit; and

the drive unit decrypts the encrypted content key received from the security module with the shared key, reads the content key-encrypted data from the optical disc ~~storage area~~ and decrypts the data.

60. (Currently Amended) The method as set forth in Claim 34, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module of the optical disc ~~data recording~~ medium;

the drive unit and the security module execute a key sharing protocol using public-key encryption technology;

the drive unit sends to the security module a content key encrypted with a shared key, and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key and records to the optical disc ~~storage area~~ the content key re-

encrypted with a save key stored in the security module and data encrypted with the content key received from the drive unit.

61. (Currently Amended) The method as set forth in Claim 34, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ via the interface unit;

the drive unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the drive unit encrypts data with a shared key and sends the data thus encrypted to the security module; and

the security module decrypts the encrypted data received from the drive unit with the shared key, encrypts the decrypted data and stores the encrypted data into the optical disc ~~storage area~~.

62. (Currently Amended) The method as set forth in Claim 34, wherein:

the drive unit is to read data from the optical disc ~~storage area~~;

the drive unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the security module reads from the optical disc ~~storage area~~ an encrypted content key and data encrypted with the content key, decrypts the encrypted content key with a save key stored therein and sends to the drive unit the content key re-

encrypted with a shared key and data encrypted with the content key read from the optical disc ~~storage area~~; and

the drive unit decrypts the encrypted content key received from the security module with the shared key and decrypts the encrypted data with the content key.

63. (Currently Amended) The method as set forth in Claim 34, wherein:

the drive unit is to read data from the optical disc ~~storage area~~;

the drive unit accesses the optical disc ~~storage area~~ via the security module;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the security module reads data encrypted and stored in the portable optical disc ~~data recording~~ medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit; and

the drive unit decrypts, with the shared key, the encrypted data received from the security module.

64. (Currently Amended) A drive unit comprising:

a controller which executes a mutual authentication protocol when accessing a portable optical disc ~~data recording~~ medium, the portable optical disc ~~data recording~~ medium including a security module comprising a nonvolatile memory and [[a]] an optical disc ~~storage area~~ distinct from the security module; and

an interface unit which accesses the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium.

wherein the mutual authentication protocol is executed by communicating with the security module of the portable optical disc medium.

65. (Previously Presented) The drive unit as set forth in Claim 64, wherein the mutual authentication protocol uses public-key encryption technology.

66. (Currently Amended) The drive unit as set forth in Claim 64, further comprising a drive means for driving ~~a disc serving as~~ the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium.

67. (Canceled)

68. (Currently Amended) The drive unit as set forth in Claim 64, wherein the interface unit accesses the optical disc ~~storage area~~ directly.

69. (Currently Amended) The drive unit as set forth in Claim 64, wherein the interface unit accesses the optical disc ~~storage area~~ via the security module.

70. (Canceled)

71. (Previously Presented) The drive unit as set forth in Claim 64, wherein the drive unit stores a revocation list of illegal recording media.

72. (Previously Presented) The drive unit as set forth in Claim 64, wherein the drive unit does not store a revocation list of illegal recording media.

73. (Currently Amended) The drive unit as set forth in Claim 64, wherein the mutual authentication protocol executes independently of whether the drive unit or the portable optical disc ~~data recording~~ medium contains an illegal unit revocation list.

74. (Canceled)

75. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive unit stores a second version of an illegal unit revocation list and a second list version number; and

the drive unit transmits, when executing the mutual authentication protocol, the second list version number to the portable optical disc ~~data recording~~ medium while receiving, from the optical disc ~~data recording~~ medium, a first list version number corresponding to a first version of the illegal unit revocation list stored by the portable optical disc ~~data recording~~ medium ~~stores~~; and

the portable optical disc ~~data recording~~ medium and the drive unit exchange the list with the newer version number.

76. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive unit stores the second list version number and the second version of the illegal unit revocation list; and

the controller transmits, when executing the mutual authentication protocol, the second list version number to the security module while receiving, from the security module, a first list version number stored in the portable optical disc ~~data recording~~ medium; and updates the second version of the illegal unit revocation list with the first version if the first version is newer than the second version.

77. (Previously Presented) The drive unit as set forth in Claim 64, wherein the drive unit stores a second version of an illegal unit revocation list to authenticate the security module and the security module stores a first version of the illegal unit revocation list to authenticate the drive unit.

78. (Currently Amended) The drive unit as set forth in Claim 75, wherein the portable optical disc ~~data recording~~ medium stores identification, and when executing

the mutual authentication protocol, the controller receives, from the security module, the identification data from the portable optical disc ~~data recording~~ medium, checks whether or not the identification data of the portable optical disc ~~data recording~~ medium is registered in the illegal unit revocation list, and will not go through subsequent processes after execution of the mutual authentication protocol if the portable optical disc ~~data recording~~ medium is revoked.

79. (Previously Presented) The drive unit as set forth in Claim 75, wherein the illegal unit revocation list includes identification data of revoked units.

80. (Previously Presented) The drive unit as set forth in Claim 75, wherein the illegal unit revocation list identifies units that have not been revoked.

81. (Previously Presented) The drive unit as set forth in Claim 75, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

82. (Previously Presented) The drive unit as set forth in Claim 64, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

83. (Previously Presented) The drive unit as set forth in Claim 64, wherein when executing the mutual authentication protocol, the drive unit and the security module execute a key sharing protocol using public-key encryption technology, encrypt a content key with a shared key and transfer the encrypted content key.

84. (Previously Presented) The drive unit as set forth in Claim 64, wherein when executing the mutual authentication protocol the drive unit and the security module executea key sharing protocol using public-key encryption technology, encrypt data with a shared key, and transfer the encrypted data.

85. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium via the interface unit;

the drive unit and the security module execute a key sharing protocol using public-key encryption technology;

the drive unit encrypts a content key with a shared key and sends the encrypted content key to the security module;

the security module decrypts the encrypted content key, re-encrypts the decrypted content key with a save key stored therein and sends the re-encrypted content key to the drive unit; and

the drive unit writes to the optical disc ~~storage area~~ of the portable optical disc ~~data recording~~ medium the data encrypted with the content key and the content key encrypted by the save key.

86. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive unit is to read data from the optical disc ~~storage area~~ via the interface unit;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the drive unit reads the encrypted content key from the optical disc ~~storage area~~ and sends the content key to the security module;

the security module decrypts the encrypted content key received from the drive unit with a save key stored therein, re-encrypts the decrypted content key with the shared key and sends the re-encrypted content key to the drive unit; and

the drive unit decrypts the encrypted content key received from the security module with the shared key, reads the content key-encrypted data from the optical disc ~~storage area~~ and decrypts the data.

87. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive unit is to write data to the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and the security module execute a key sharing protocol using public-key encryption technology;

the drive unit sends to the security module a content key encrypted with a shared key, and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key and records to the optical disc ~~storage area~~ the content key re-

encrypted with a save key stored in the security module and data encrypted with the content key received from the drive unit.

88. (Currently Amended) The drive unit as set forth in Claim 64, wherein

the drive unit is to write data to the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the drive unit encrypts data with a shared key and sends the data thus encrypted to the security module; and

the security module decrypts the encrypted data received from the drive unit with the shared key, encrypts the decrypted data and stores the encrypted data into the optical disc ~~storage area~~.

89. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive unit is to read data from the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module of the portable optical disc ~~data recording~~ medium;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the security module reads from the optical disc ~~storage area~~ an encrypted content key and data encrypted with the content key, decrypts the encrypted content key with a save key stored therein and sends to the drive unit the content key re-

encrypted with a shared key and data encrypted with the content key read from the optical disc ~~storage area~~; and

the drive unit decrypts the encrypted content key received from the security module with the shared key and decrypts the encrypted data with the content key.

90. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive unit is to read data from the optical disc ~~storage area~~ via the interface unit;

the interface unit accesses the optical disc ~~storage area~~ via the security module;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the security module reads data encrypted and stored in the portable optical disc ~~data recording~~ medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit; and

the drive unit decrypts, with the shared key, the encrypted data received from the security module.

91-114. (Canceled)

115. (Withdrawn) A data recording medium having a data recording area, comprising:

a security module having an interface function for interfacing with an external unit, a random number generating function, a data storing function, and a calculating function to provide a necessary calculation for mutual authentication protocol using the public-key encryption technology; and

a recording medium proper having the data recording area.

116. (Withdrawn) The data recording medium as set forth in Claim 115, wherein the security module further includes an interface function to access the data recording medium proper.

117. (Withdrawn) An access method for access to a data recording medium having a data recording area, the method comprising steps of:

connecting to an external unit;

generating a random number and sending it to the external unit;

making, using data received from the external unit and stored data, a necessary calculation for a protocol, for mutual authentication with the external unit, using the public-key encryption technology;

executing the mutual authentication mutual authentication protocol with the external unit; and

accessing a recording medium proper, in which data is to be recorded, of the data recording medium according to the result of the mutual authentication protocol execution.

118. (Withdrawn) A recording medium producing apparatus for producing a data recording medium, comprising:

a recording unit to record an illegal unit revocation list to the data recording medium which includes a recording medium proper in which data is to be recorded and a security module which executes a mutual authentication mutual authentication protocol with a drive unit which accesses the recording medium proper of the data recording medium.

119. (Withdrawn) The unit as set forth in Claim 118, further comprising an assembling unit to assemble the data recording medium including the security module and recording medium proper.

120. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list into the security module.

121. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list version number and the list itself into the security module.

122. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list in the recording medium proper.

123. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list version number into the security module and the list itself in the recording medium proper.

124. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records, into the security module, the identification data of the data recording medium, private key and public key certificates which are to be used in the public key encryption technology given in the data recording medium, and the list version number.

125. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit further comprises means for storing the list which is to be recorded to the data recording medium.

126. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit further comprises an interface through which the list to be recorded into the data recording medium is acquired.

127. (Withdrawn) The unit as set forth in Claim 118, wherein the list is composed of a revocation list having registered therein identification data of units having to be revoked and/or a registration list having registered therein identification data of units having not to be revoked.

128. (Withdrawn) A recording medium producing method for producing a data recording medium, comprising a step of:

recording an illegal unit revocation list to the data recording medium which includes a recording medium proper in which data is to be recorded and a security module which executes a mutual authentication mutual authentication protocol with a drive unit which accesses the recording medium proper of the data recording medium.

129. (Withdrawn) The method as set forth in Clam 128, in which the data recording medium including the security module and recording medium proper is assembled.

130. (Withdrawn) The method as set forth in Claim 128, wherein the list is recorded into the security module.

131. (Withdrawn) The method as set forth in Claim 128, wherein the list version number and the list itself are recorded into the security module.

132. (Withdrawn) The method as set forth in Claim 128, wherein the list is recorded to the recording medium proper.

133. (Withdrawn) The method as set forth in Claim 128, wherein the list version number is recorded into the security module while the list itself is recorded to the recording medium proper.

134. (Withdrawn) The method as set forth in Claim 128, wherein the identification data of the data recording medium, private and public key certificates which are to be used in the public-key encryption technology given in the data recording medium, and the list are recorded into the security module.

135. (Withdrawn) The method as set forth in Claim 128, wherein the list is stored into the data recording medium.

136. (Withdrawn) The method as set forth in Claim 128, wherein the list to be recorded into the data recording medium is acquired from outside.

137. (Withdrawn) The method as set forth in Claim 128, wherein the list is composed of a revocation list having registered therein units having to be revoked and/or a registration list having registered therein units having not to be revoked.

138. (Previously Presented) The system as set forth in Claim 20, wherein the illegal unit revocation list includes identification data of revoked units.

139. (Previously Presented) The system as set forth in claim 21, wherein the illegal unit revocation list includes identification data of revoked units.

140. (Previously Presented) The system as set forth in Claim 20, wherein the illegal unit revocation list identifies units that have not been revoked.

141. (Previously Presented) The system as set forth in Claim 21, wherein the illegal unit revocation list identifies units that have not been revoked.

142. (Previously Presented) The system as set forth in Claim 20, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

143. (Previously Presented) The system as set forth in Claim 21, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

144. (Previously Presented) The system as set forth in Claim 20, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

145. (Previously Presented) The system as set forth in Claim 21, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units ; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

146. (Previously Presented) The method as set forth in Claim 50, wherein the illegal unit revocation list includes identification data of revoked units.

147. (Previously Presented) The method as set forth in Claim 51, wherein the illegal unit revocation list includes identification data of revoked units.

148. (Previously Presented) The method as set forth in Claim 50, wherein the illegal unit revocation list identifies units that have not been revoked.

149. (Previously Presented) The method as set forth in Claim 51, wherein the illegal unit revocation list identifies units that have not been revoked.

150. (Previously Presented) The method as set forth in Claim 50, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

151. (Previously Presented) The method as set forth in Claim 51, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

152. (Previously Presented) The method as set forth in Claim 50, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

153. (Previously Presented) The method as set forth in Claim 51, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

154. (Previously Presented) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list includes identification data of revoked units.

155. (Previously Presented) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list includes identification data of revoked units.

156. (Previously Presented) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list includes:

a revocation list identifying revoked units; and

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked.

157. (Previously Presented) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list includes:

a revocation list indicating revoked units; and

a registration list indicating units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked.

158-161. (Canceled)

162. (Withdrawn) A storage apparatus for storing information retrieved by an information processing apparatus, the storage apparatus comprising:

a storage section for storing a first revoked unit list;

a receiving section for receiving a second revoked unit list from the information processing apparatus; and

a judging section for judging whether the information processing apparatus is revoked or not based on the first revoked unit list;

wherein if the information processing apparatus is revoked, the first revoked unit list is maintained, and if the information processing apparatus is not revoked, the first revoked unit list is replaced with the second revoked unit list.

163. (Withdrawn) The storage apparatus as set forth in Claim 162, further comprising a receiving section for receiving ID information from the information processing apparatus.

164. (Withdrawn) The storage apparatus as set forth in Claim 163, wherein the ID information includes a key for the information processing apparatus.

165. (Withdrawn) The storage apparatus as set forth in Claim 164, wherein a digital certification includes the key.

166. (Withdrawn) The storage apparatus as set forth in Claim 162, wherein the judging section judges whether the information processing apparatus is on the first revoked unit list.

167. (Withdrawn) The storage apparatus as set forth in Claim 162, further comprising:

a comparing section for comparing the first revoked unit list with the second revoked unit list; and

a second judging section for judging which revoked unit list is newer.

168. (Withdrawn) The storage apparatus as set forth in Claim 167, further comprising:

a transmitting section for transmitting the first revoked unit list to the information processing apparatus.

169. (Withdrawn) The storage apparatus as set forth in Claim 167, wherein the second judging section compares the respective version information attached with each revoked unit list.

170. (Withdrawn) The storage apparatus as set forth in Claim 162, further comprising:

a second receiving section for receiving a private key from the information processing apparatus;

a second storage section for storing a public key; and

a judging section for judging whether the private key and the public key correspond.

171. (Withdrawn) The storage apparatus as set forth in Claim 170, wherein if the information processing apparatus is revoked or the private key does not relate to the public key, the first revoked unit list is maintained, and if the information processing

apparatus is not revoked and the private key relates to the public key, the first revoked unit list is replaced with the second revoked unit list.

172. (Withdrawn) The storage apparatus as set forth in Claim 171, wherein if the first revoked unit list is maintained and the information processing apparatus is not revoked, the first revoked unit list is transmitted to the information processing apparatus.

173. (Withdrawn) The storage apparatus as set forth in Claim 162, wherein the storage section comprises:

a revoked unit list storage section for storing the first revoked unit list; and

a content storage section for storing content.

174. (Withdrawn) The storage apparatus as set forth in Claim 173, wherein the revoked unit list storage section is more secure than the content storage section.

175. (Withdrawn) The storage apparatus according to claim 162, wherein the first revoked unit list indicates at least one information processing apparatus whose private key has been revealed.

176. (Withdrawn) The storage apparatus according to claim 162, wherein the storage apparatus and the information processing apparatus share a common private key.

177. (Withdrawn) An information processing apparatus for retrieving information from a storage apparatus, comprising:

a storage section for storing a second revoked unit list;

a receiving section for receiving a first revoked unit list from the storage apparatus; and

a judging section for judging whether the storage apparatus is revoked or not based on the second revoked unit list;

wherein if the storage apparatus is revoked, the second revoked unit list is maintained, and if the storage apparatus is not revoked, the second revoked unit list is replaced with the first revoked unit list.

178. (Withdrawn) The information processing apparatus as set forth in Claim 177, further comprising a receiving section for receiving ID information from the storage apparatus.

179. (Withdrawn) The information processing apparatus as set forth in Claim 178, wherein the ID information includes a key for the storage apparatus.

180. (Withdrawn) The information processing apparatus as set forth in Claim 179, wherein a digital certification includes the key.

181. (Withdrawn) The information processing apparatus as set forth in Claim 177, wherein the judging section judges whether the storage apparatus is on the second revoked unit list.

182. (Withdrawn) The information processing apparatus as set forth in Claim 177, further comprising:

a comparing section for comparing the first revoked unit list with the second revoked unit list; and

a second judging section for judging which revoked unit list is newer.

183. (Withdrawn) The information processing apparatus as set forth in Claim 182, further comprising a transmitting section for transmitting the second revoked unit list to the storage apparatus.

184. (Withdrawn) The information processing apparatus as set forth in Claim 182, wherein the second judging section compares the respective version information attached with each revoked unit list.

185. (Withdrawn) The information processing apparatus as set forth in Claim 177, further comprising:

a second receiving section for receiving a private key from the storage apparatus;

a second storage section for storing a public key; and

a judging section for judging whether the private key and the public key correspond.

186. (Withdrawn) The information processing apparatus as set forth in Claim 185, wherein if the storage apparatus is revoked or the private key does not relate to the public key, the second revoked unit list is maintained, and if the storage apparatus is not revoked and the private key relates to the public key, the second revoked unit list is replaced with the first revoked unit list.

187. (Withdrawn) The information processing apparatus as set forth in Claim 186, wherein if the second revoked unit list is maintained and the storage apparatus is not revoked, the second revoked unit list is transmitted to the storage apparatus.

188. (Withdrawn) The information processing apparatus as set forth in Claim 177, wherein the storage section comprises:

a revoked unit list storage section for storing the second revoked unit list; and

a content storage section for storing content.

189. (Withdrawn) The information processing apparatus as set forth in Claim 188, wherein the revoked unit list storage section is more secure than the content storage section.

190. (Withdrawn) The information processing apparatus as set forth in Claim 177, further comprising a playing back section for playing back information retrieved from the storage apparatus.

191. (Withdrawn) The information processing apparatus according to claim 177, wherein the second revoked unit list indicates at least one storage apparatus whose private key has been revealed.

192. (Withdrawn) The storage apparatus according to claim 177, wherein the storage apparatus and the information processing apparatus share a common private key.

193. (Withdrawn) A system comprising an information processing apparatus and a storage apparatus, the information processing apparatus comprising:

a storage section for storing a second revoked unit list;

a receiving section for receiving a first revoked unit list from the storage apparatus; and

a judging section for judging whether the storage apparatus is revoked or not based on the second revoked unit list;

wherein if the storage apparatus is revoked, the second revoked unit list is maintained in the information processing apparatus, and if the storage apparatus is not revoked, the second revoked unit list is replaced with the first revoked unit list in the information processing apparatus; and

the storage apparatus comprising:

a storage section for storing the first revoked unit list;

a receiving section for receiving the second revoked unit list from the information processing apparatus; and

a judging section for judging whether the information processing apparatus is revoked or not based on the first revoked unit list;

wherein if the information processing apparatus is revoked, the first revoked unit list is maintained in the storage apparatus, and if the information processing apparatus is not revoked, the first revoked unit list is replaced with the second revoked unit list in the storage apparatus.

194. (Withdrawn) The system as set forth in Claim 193, the information processing apparatus further comprising a receiving section for receiving ID information from the storage apparatus.

195. (Withdrawn) The system as set forth in Claim 194, wherein the ID information is a key for the storage apparatus.

196. (Withdrawn) The system as set forth in Claim 195, wherein a digital certification includes the key.

197. (Withdrawn) The system as set forth in Claim 193, wherein the judging section for judging whether the storage apparatus is revoked judges whether the storage apparatus is on the second revoked unit list.

198. (Withdrawn) The system as set forth in Claim 193, the information processing apparatus further comprising:

a comparing section for comparing the first revoked unit list with the second revoked unit list; and

a second judging section for judging which revoked unit list is newer.

199. (Withdrawn) The system as set forth in Claim 198, the information processing apparatus further comprising a transmitting section for transmitting the second revoked unit list to the storage apparatus.

200. (Withdrawn) The system as set forth in claim 198, wherein the second judging section compares the respective version information attached with each revoked unit list.

201. (Withdrawn) The system as set forth in Claim 193, the information processing apparatus further comprising:

a second receiving section for receiving a private key from the storage apparatus;

a second storage section for storing a public key; and

a judging section for judging whether the private key and the public key correspond.

202. (Withdrawn) The system as set forth in Claim 201, wherein if the storage apparatus is revoked or the private key does not relate to the public key, the second revoked unit list is maintained, and if the storage apparatus is not revoked and the private key relates to the public key, the second revoked unit list is replaced with the first revoked unit list.

203. (Withdrawn) The system as set forth in Claim 202, wherein if the second revoked unit list is maintained and the storage apparatus is not revoked, the second revoked unit list is transmitted to the storage apparatus.

204. (Withdrawn) The system as set forth in Claim 193, wherein the storage section for storing the second revoked unit list comprises:

a revoked unit list storage section for storing the second revoked unit list; and

a content storage section for storing content.

205. (Withdrawn) The system as set forth in Claim 204, wherein the revoked unit list storage section is more secure than the content storage section.

206. (Withdrawn) The system set forth in Claim 193, the information processing apparatus further comprising a playing back section for playing back information retrieved from the storage apparatus.

207. (Withdrawn) The system according to claim 193, wherein the second revoked unit list indicates at least one storage apparatus whose private key has been revealed.

208. (Withdrawn) The system according to claim 193, wherein the storage apparatus and the information processing apparatus share a common private key.

209. (Withdrawn) A method for retrieving information from a storage apparatus, comprising:

storing a second revoked unit list;

receiving a first revoked unit list from the storage apparatus; and

judging whether the storage apparatus is revoked or not based on the second revoked unit list;

wherein if the storage apparatus is revoked, the second revoked unit list is maintained, and if the storage apparatus is not revoked, the second revoked unit list is replaced with the first revoked unit list.

210. (Withdrawn) The method as set forth in Claim 209, further comprising receiving ID information from the storage apparatus.

211. (Withdrawn) The method as set forth in Claim 210, wherein the ID information includes a key for the storage apparatus.

212. (Withdrawn) The method as set forth in Claim 211, wherein a digital certification includes the key.

213. (Withdrawn) The method as set forth in Claim 209, wherein judging whether the storage apparatus is revoked includes judging whether the storage apparatus is on the second revoked unit list.

214. (Withdrawn) The method as set forth in Claim 209, further comprising:

comparing the first revoked unit list with the second revoked unit list; and

judging which revoked unit list is newer.

215. (Withdrawn) The method as set forth in Claim 214, further comprising transmitting the second revoked unit list to the storage apparatus.

216. (Withdrawn) The method as set forth in claim 214, further comprising comparing the respective version information attached with each revoked unit list.

217. (Withdrawn) The method as set forth in Claim 209, further comprising:

receiving a private key from the storage apparatus;

storing a public key; and

judging whether the private key and the public key correspond.

218. (Withdrawn) The method as set forth in Claim 217, wherein if the storage apparatus is revoked or the private key does not relate to the public key, the second revoked unit list is maintained, and if the storage apparatus is not revoked and the private key relates to the public key, the second revoked unit list is replaced with the first revoked unit list.

219. (Withdrawn) The method as set forth in Claim 218, wherein if the second revoked unit list is maintained and the storage apparatus is not revoked, the second revoked unit list is transmitted to the storage apparatus.

220. (Withdrawn) The method as set forth in Claim 209, further comprising storing content.

221. (Withdrawn) The method as set forth in Claim 220, wherein the revoked unit list is stored more securely than the content.

222. (Withdrawn) The method set forth in Claim 209, further comprising playing back information retrieved from the storage apparatus.

223. (Withdrawn) The method according to claim 209, wherein second revoked unit list indicates at least one storage apparatus whose private key has been revealed.

224. (Withdrawn) The method according to claim 209, wherein the storage apparatus and the information processing apparatus share a common private key.